A protocolized, comparative study of Helios Voting and Scytl/iVote

David Yeregui Marcos del Blanco* and Mila Gascó†
*University of León
León, Spain
Email: david.yeregui.marcos@gmail.com
†CTG UAlbany
University at Albany
Suny, United States
Email: mgasco@ctg.albany.edu

***Abstract*— E-voting implantation is happening at a slower pace than anticipated. A plethora of technical and social challenges hinder a deeper implementation. In this article, the problem is addressed by applying a practical evaluation framework to two of the most relevant e-voting tools: Helios Voting and iVote from Scytl. The framework is strongly based on the technical requirements issued by the Council of Europe in 2017.The authors believe it can constitute a useful source of information for election officials, researchers and even voters. The final purpose is contributing to a gradual, secure and protocolized expansion of e-voting in Europe; more so in the present times, with mounting geo-political challenges and tensions.**

Keywords—Internet Voting, evaluation, Helios Voting, Scytl

I. INTRODUCTION

The Information and Communications Technologies (ICT) have had a huge impact in the way humans interact with their environment. In the early 2000s, it was widely anticipated that its range would also include public elections and other democratic processes, as an integral part of what was labeled as e-democracy.

More than a decade after, that promise has not been fulfilled although countries like Estonia, Australia, Norway, Switzerland or Canada have implemented e-voting pilots for binding elections totaling more than 6 million votes. Currently, only Estonia has introduced e-voting for every election and the whole census. However, there have been reported security issues, which might have jeopardized the results [1] .

Certainly, e-voting introduces features making it an especially demanding discipline within the plethora of ICT applications [2]:

- The requirement to comply with two opposed properties: integrity and privacy.
- The results are almost impossible to revert when an attack is discovered after the elections ended.
- The existence of a traditional voting system which is simple, intuitive, verifiable and offering reasonably satisfactory results.

Another hindrance are the three main attack vectors:

- The voter's device, with a 30-40% prevalence of malware and situated in uncontrolled environments [2].
- The network, with a well documented track record of attacks on the associated cryptographic protocols [3].
- The e-voting system itself, potentially incorporating vulnerabilities/bugs able to put the elections in jeopardy[1, 4].

The examples of attacks coming from foreign nations during e-voting pilots in the past in countries like US and Australia among others [5] remind us of the utmost importance of constantly improve security measures and remain vigilant.

Despite the relevance of security in e-voting processes and the growing international risks, the evaluation of e-voting systems, is still an important challenge, only a few works have addressed. In 2015, the IEEE reactivated the 1622 Committee on Voting System Standards [6], but it only included a set of recommendations. In 2016, Neumann proposed a probabilistic framework for e-voting schemes [7]. Subsequently, Panizo et al. introduced a comprehensive methodology with technical and legal re-marks as well as practical recommendations in their evaluation system presented in the Ph. D. chapter of the E-Vote-ID 2016 conference [8]. In particular, they considered the Council of Europe e-voting requirements [9], as well as a set of 73 technical and practical factors evaluated by 21 international experts in the e-voting field [10].

In the present article, the authors apply the framework in [8] to two of the most relevant e-voting tools: Helios Voting [11] implemented by Harvard researcher Dr. Ben Adida and the iVote system developed by the company Scytl [12]. The present article's scope is limited to the evaluation of only two systems due to page limitation. The authors are currently working on further comparative studies with other e-voting solutions.

II . RELATED WORKS

One of the most relevant research to date belongs to Bräunlich [13], in which the first interdisciplinary study to transform legal requirements into technical criteria was presented. In particular, the authors came up with thirty Technical Design Goals (TDG), built upon the KORA method [14].

Based on [13], Neumann, from TU Darmstadt, combined [13] with the Common Criteria for IT-Security Evaluation [15] and defined sixteen technical requirements to link the legal criteria with Bräunlich's TDGs. Neumann's research [7] crucially contributes to building a valid framework, while it still presents room for improvement:

- The security evaluation is based on voters sufficiently utilizing verification tools. Unfortunately, experience has shown otherwise: in one of the biggest initiatives to date in New South Wales in 2015, only a 1.7% of 283.669 votes were verified [16].

978-1-7281-1704-1/19/$31.00 © 2019 IEEE

- It is based on probabilistic attack strategies applying Monte-Carlo simulations. It is indeed a very interesting approach, but Neumann concludes *"we recommend to incorporate the security evaluation framework into a larger decision-support system for elections officials"* [10, p. 138].

III. EVALUATION METHODOLOGY

Bräunlich et al. [13] greatly contributed to the evaluation of e-voting systems by introducing the first transformation of election principles into technical design goals (TDG).

Subsequently, Neumann [7] identified the shortcomings in [13] and proposed a number of technical requirements to link legal criteria with Bräunlich's TDGs.

While Neumann introduced undeniable improvements, it was still a scheme evaluation tool based on Monte-Carlo simulations rather than a practical framework to pro-vide evaluation information for election officials. The author stated in the conclusion that: "we therefore recommend to incorporate the security evaluation framework into a larger decision-support system for elections officials" [14, p. 138].

Building on Neumann's conclusion, Panizo, et al. presented a proposal of a decision-support system in the form of a practical evaluation framework [8]. It is compliant with the 2017 Council of Europe' guidelines ("Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting") [9]. The proposed comprehensive evaluation framework [8], includes the following steps:

1. Definition of an homogeneous set of e-voting requirements based on: KORA [14], CC and ISO 27001-IT Grundschutz [15], their integration by Simic-Draws et al. [17], the Council of Europe Guidelines [9] and Neumann's methodology [7].
2. Formal equivalence between point 1 and Bräunlich [13] as shown below in Fig. 1.
3. Consultation with more than 30 international experts in e-voting (Research and Industry Experts or RIE, selected using the snowball [18] and judgement [19] sampling methodologies) to review the evaluation framework and add weighting factors.
4. Formal definition of the practical evaluation framework, including two sine-qua-non requirements (E2Ev and Coercion Resistance) and 73 evaluation items.

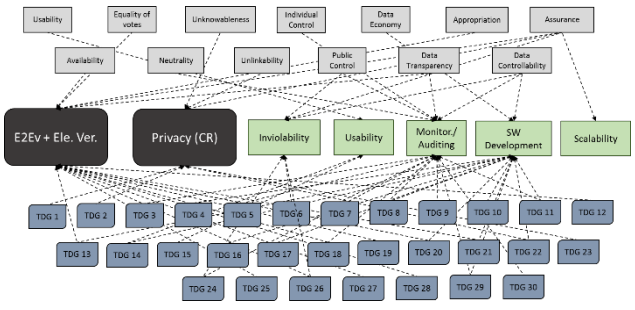

Fig. 1. Integration of Bräunlich [13] and Panizo [8]

The previous system, while sound from a legal point of view, presents similar limitations to Neumann's methodology [7] given the lack of coverage of many of the technical and practical aspects of a complete e-voting system.

As a result, an additional set of five requirements for e-voting systems was included partially based on the research by Benaloh, Rivest, Ryan and Volkamer [20], [21]. Finally, all the requirements were codified, refined and itemized into 73 specific items by partially applying Zissis and Lekkas [22] and New Zealand's Department of Internal Affair's Report on e-voting [23].

Fig. 2 represents the complete scheme of the evaluation framework:

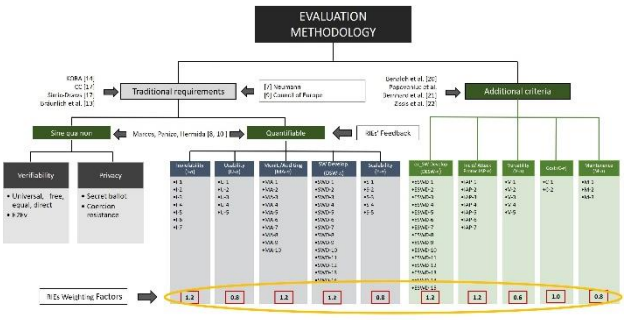

Fig. 2. Complete practical evaluation framework [8]

Fig. 2 shows that there are two types of criteria: The sine-qua-non one, for which end-to-end verifiability and coercion resistance [24], [25] represent the five mandatory principles of a democratic election (Council of Europe [9]). In this case, the evaluation is not a numerical value related to performance but rather as "holds" (○), "does not hold" (×) or "holds under certain, plausible assumptions" (Δ).

The second set includes the quantifiable traditional requirements and the additional criteria. They are evaluated from 0 to 10 with a one decimal accuracy. In order to calculate the numerical value, each of the 73 measurable items are reviewed as: non-compliant (×), partially compliant (Δ) and compliant (○).

IV. EVALUATION

In this section, we analyze the official version of Helios Voting [26] and the iVote system developed by the company Scytl SA [12]. More recent versions of Helios such as KTV-Helios [27] have not yet been fully deployed in binding elections and therefore the evaluation framework cannot be entirely applied.

Helios Voting [11] is a free, open-source, web-based e-voting system developed by Adida. It has been used in several relevant elections, as in the University of Louvain [28], and the International Association of Cryptologic Research [29]. Altogether, more than 100,000 votes have been cast with Helios. It is widely considered the cornerstone in open-source e-voting and one of the main references to develop new systems. From a cryptographic standpoint, Helios exploits the additive homomorphic and distributed decryption properties of ElGamal and Sako-Killian's mixnet protocol, and uses the Chaum-Pedersen protocol as a proof of decryption. For a complete explanation of Helios Voting protocol, please refer to [11].

As for Scytl, it is a world leader in election solutions based in Barcelona. It was founded in 2001 and currently employs over 250 people. They have managed over 100,000 electoral events across more than 20 countries. They own more than 40

1. For a complete explanation of the methodology, the definition of the sine-qua-non, re-quirements and the 73 evaluation items, refer to the original work in [8], [10].

inter-national patents in the area of security applied to election processes. Depending on the applicable jurisdiction and election typology of each country, Scytl adapts the iVote tool from a design and cryptographic standpoints to the specific requirements. In this section, the authors consider the best performing iVote version for each evaluated item.

A. End to End verifiability

Names should not be listed in columns nor group by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization).

Currently, there does not exist a formal, universal definition for E2Ev because associative and commutative operators are out of reach for symbolic analysis tools, making it impossible for example to analyze the following homomorphic property as pointed out in [30]:

$$enc\,(pk;1) * enc(pk;v2) = enc\;(pk;v1+v2) \qquad (1)$$

Therefore, the challenge of formally defining verifiability remains unresolved, which results in case by case analyses. The most accepted definition of E2Ev is comprised of three well known properties [20]: cast as intended, recorded as cast and tallied as recorded.

Helios introduces the cast-or-audit approach for the cast as intended property: the voter can audit her vote as many times as she wants, until she is convinced that Helios is trustable. For recorded as cast, the voter receives a hash of her encrypted vote, which can later check on the bulletin board. Finally, for the tallied as recorded condition, ElGamal together with the Sako-Kilian mixnet [31] are implemented with a Zero Knowledge Proof (ZKP). As a consequence, Adida concludes that Helios is E2Ev [11] if both the bulletin board and the election authorities are honest. Otherwise, any of these two parties could irregularly add votes ("ballot stuffing"). Newer versions such as KTV-Helios [27] have improved E2Ev by requiring that only the bulletin board or the authorities be honest.

Regarding iVote, for E2Ev analysis we consider the system deployed in the Norwegian elections. Both the Carter Center [32] and Gjøsteen [33] explained that, despite the fact that the Norwegian authorities didn't demand the system to be E2Ev, the individual and proxy verifiability, together with the ZKPs and the publicly-accessible Github Bulletin Board conformed an overall verifiable tool. The only condition was that there was no collusion among the code-generator, the authentication service and the electoral letter generator, which in practice is very unlike given the role distribution, together with the independent auditing.

Evaluation Helios: Δ. E2Ev holds under certain, plausible assumptions.

Evaluation iVote: Δ. E2Ev holds under certain, plausible assumptions.

B. Coercion Resistance

Headings, According to Juels definition [25], coercion resistance is the most demanding version of privacy, as it establishes that a voter cannot prove to a coercer that she has voted in a certain way, even if she is willing to). Hirt and Sako proved in [34] that the previous level (receipt-freeness) is not enough for electronic elections.

Concerning Helios and according to Adida: "*with Helios, we do not try to solve the coercion problem" and "privacy is ensured by recruiting enough trustees*" (p. 1). Despite this statement, ballot privacy attacks on Helios have been documented [4].

In Australia, the authorities do not consider coercion as a relevant risk and there-fore it is not taken into account for iVote. Regarding Neuchâtel and Norway, the re-turn codes have several security advantages but they compromise coercion resistance.

Evaluation Helios: X. Does not hold in Helios Voting.
Evaluation iVote: X. Does not hold in iVote.

C. Inviolability (I-n)

Helios allows identification through third parties, failing to comply with I-1. Similarly, it does not include tracking tools, offline backups, risk assessment or threat modelling protocols (I-3, I-5). Regarding I-2, I-4 and I-6, there is a brief Attacks and Defenses section in the official website and distributed policies have been implemented together with modularity principles. Finally, the open source approach and Adida's eagerness to help scholars improve Helios [27] makes Helios compliant for I-7.

Concerning iVote, the Australian version was vulnerable to FREAK [3] (although not because of a flaw in the system, but through an external analysis tool). Also, during the Norwegian pilots, there was a reported bug in ElGamal, which was immediately repaired. Subsequent elections in Neuchâtel have concluded with no issues, suggesting an overall improvement in inviolability for Scytl's e-voting tool.

TABLE I. INVIOLABILITY IN HELIOS AND IVOTE

I-n	Definition	H	S
I-1	Software and auxiliary system's protection w/ safe authentication protocols. Access via third-parties/vulnerable-servers not permitted.	X	Δ
I-2	Action protocols in the event of compromised inviolability.	Δ	○
I-3	Tracking tools and offline backup copies available.	X	○
I-4	Distributed control in the critical nodes with division of responsibilities to minimize collusion risks.	Δ	Δ
I-5	Existence of *Risk Assessment* and *Threat Modelling* protocols.	X	Δ
I-6	Modularity principles to confine potential attacks and coding bugs.	Δ	Δ
I-7	Proper updating of items I-1…I-6	○	○

Evaluation Helios: 6/10 points. Adida stated that Helios is suitable for minor elections in low-coercion/low-risk environments. In such case, it shows a fair level of inviolability.

Evaluation iVote: 8/10 points. iVote's inviolability policy includes action protocols, tracking tools, backup copies and a good update policy. It has been taken into account that Scytl's voting tool has been analyzed (unlike Helios) for legally-binding public elections, the most demanding typology for complexity and security reasons.

D. Usability (U-n)

There has been relevant articles studying Helios' such as [35] showing that: 1) the terminology is somehow misleading, 2) the help button is insufficient, 3) the cast or audit approach is not intuitive, leading to a 38% of voters not successfully casting their ballot. Nonetheless, over 85% of the users felt very comfortable using Helios. Overall, Helios performance with regards to (U1-U5) is below average. Fortunately, some

of the deficiencies can be addressed paying closer attention to detail, without big investments.

As for iVote, in Australia the satisfaction rate is currently 95%, and in Norway there was a demanding "Accessibility and Usability" chapter in the tender as well as a Voter Information Center ready to solve questions and usability issues. Finally, Scytl implemented a usability layer to reduce the length of the codes to be stored by the voter.

TABLE II. USABILITY IN HELIOS AND IVOTE

U-*n*	Definition	H	S
U-1	Simplicity in the authentication, voting and verification	Δ	Δ
U-2	Special attention to vulnerable groups pursuant to the Council of Europe and the United Nations' resolutions on the matter.	X	Δ
U-3	Transparency & clarity communicating the voter that the voting process has successfully ended/ vote has been received.	Δ	○
U-4	Privacy and integrity preference over usability in a compromise.	Δ	○
U-5	Intuitive/user-friendly administration interface for setup and management.	Δ	Δ

Evaluation Helios: 4/10 points.

Evaluation iVote: 7.5/10 points. iVote has gradually improved the usability with specific chapters, Information Centers and intermediate layers. Nonetheless, one of Scytl's researchers has pointed out that there is still room for improvement [36], since the voter is still required to store codes, messages and sometimes even printed code letters.

E. Monitoring/Auditing (MA-n)

In Helios, there is no specific MA protocol, thus several of the items are no applicable. MA-1, MA-4, MA-5 and MA-8 are partially compliant because they were de-ployed in a very specific Helios pilot (the election of the President of the University of Louvain [28]), although those items are not available in the standard version [26].

Concerning iVote, it has been deployed in public binding elections in countries with a long and stable democratic tradition like Australia, Switzerland or Norway. Thus, the official tenders included close monitoring and auditing from independent companies/experts (sometimes even the companies who lost the same tender) [37, 38].

Evaluation Helios: 3/10 + 1 extra point. Helios audit is based on facilitating the auditing of the individual/universal verifiability rather than implementing a solid and independent proto-col. The extra point is awarded because Helios was originally created for small-scale, low-risk contexts. In such cases, although insufficient, the MA policy could be acceptable.

Evaluation iVote: 8.5/10 points. iVote has been deployed for binding political elections, in stable countries with enough financial and human resources so the outcome has been highly satisfactory. Improvable aspects include early error detection and better time allocation to avoid last-minute rushes.

TABLE III. MA PROTOCOLS

MA-*n*	Definition	H	S
MA-1	External, independent and distributed.	Δ	○
MA-2	MA protocol from the design phase, to assure a correct development throughout the whole lifecycle of the project.		○
MA-3	*Specific control on Risk Assess.* and *Thread Modelling strategies.*		○
MA-4	Generation of periodical, tamper-proof, indelible logs; stored offline in premises guarded by different personnel from other critical nodes.	Δ	Δ
MA-5	Practical implementation from census collecting to post-electoral maintenance.	Δ	○
MA-6	Well-documented, detailed information in the appropriate format.	Δ	○
MA-7	Existence of a test bench to verify that the system is working correctly.		
MA-8	The members of the monitoring/auditing team must be independent from the rest of authorities/administrators involved.	Δ	○
MA-9	Auditing protocol for previous attacks and for the MA protocol itself.		○
MA-10	In the event of a successful attack, the system will give total priority to the vote/voter's privacy, even calling off the elections.		

F. Software Development (SWD-n)

Since its inception in 2008, Helios has gathered attention from cryptography, cybersecurity and e-democracy researchers who have thoroughly reviewed the (open source) code [39, 27, 40]. As a consequence, Helios' software is compliant with items SWD-1, SWD-4, SWD-5, SWD-7, SWD-8, SWD-11, SWD-12 and SWD-13. Software testing in systems/browsers with a market share $\geqslant$ 1% (SWD-9) still shows weak-nesses, as does the access through third-parties (SWD-10) and the update policy (SWD-14). Finally, the distributed approach (SW-2) and usability (SW-3) have only been partially developed.

Regarding iVote, the experience amassed by Scytl during the last 15 years with a team of over 250 people in legally-binding political elections has refined a software that has been made available for the Norwegian e-voting project in 2011-2013. It is compliant with items SWD-1, SWD-2, SWD-4, SWD-5, SWD-7-SWD-9 and SWD-11. SWD-12 and SWD-14. There is room for improvement in user-friendly approach (SWD-3), receipt-free solutions (SWD-6) and third party access.

Evaluation Helios: 7.5/10 points. Helios presents a satisfactory degree of software development, considering its academic origins and the limited resources. Yet, there is room for improvement in usability, distributed approach, access through third-parties and updating.

Evaluation iVote: 8.5/10 points. Scytl's experience and resources have contributed to the development of a very solid software in terms of design, development and documentation. Pending issues include third party access, a better user experience, receipt-free alternatives and a further implementation of open standards to improve interoperability

TABLE IV. SOFTWARE DEVELOPMENT IN HELIOS AND IVOTE

SWD-*n*	Definition	H	S
SWD-1	Usual software engineering requirements in terms of design, implementation and documentation.	○	○
SWD-2	Distributed approach on critical operations. No authority should have attributions to single-handedly modify critical parameters.	Δ	○
SWD-3	User-friendly approach. User's guide and administrator's guide well documented and available well in advance.	Δ	Δ
SWD-4	Secure and accessible website, with a well-documented FAQ section.	○	○
SWD-5	The voting options must be presented in a totally objective and unbiased way, showing no preference whatsoever.	○	○
SWD-6	System must not provide the voter with evidence to proof her vote.	Δ	Δ
SWD-7	The system must guarantee the voter's privacy throughout the whole voting process, not being possible to rebuild the vote/voter link.	○	○
SWD-8	The voting process must offer the possibility to be terminated at any time, not saving any information compromising the voter's privacy.	○	○
SWD-9	SW to be tested in every platform, operational system and browser with a market share ≥ 1%.	X	○
SWD-10	Software must neither allow for third-party access (incl. social media) nor include links to programs/sites outside the e-voting infrastructure.	X	Δ
SWD-11	The cryptographic primitives shall be tested in advance under conditions more demanding than the ones expected during the elections in order to avoid breakdowns and foresee shortages.	○	○
SWD-12	Access to the source code by independent experts to reinforce security. The code developer can demand an NDA to protect its IP.	○	○
SWD-13	Use of protocolized systems/open standards to improve interoperability.	○	Δ
SWD-14	Update policy, against new e-voting attacks as they are discovered.	X	○

G. Scalability

Helios's origin and academic nature have great impact on the available resources for development and updating, as we have just shown. They also limit the ability to undertake capacity and performance tests, and attack simulations (S-1, S-2 and S-3). Regarding E-4 and E-5, the official documentation does not specify a concrete figure. Previous pilots have shown that the standard version has managed around 1.000 ballots [29] and the reinforced version in Lovain [28] two rounds of 3.000 ballots each. As for the typology, Helios utilization is recommended in the case of small scale, low-risk elections.

On the contrary, iVote has been used numerous occasions in some of the biggest e-voting pilots up to hundreds of thousands of voters without capacity issues. Regarding election type, Scytl's experience includes the most demanding one: legally-binding public elections.

TABLE V. SCALABILITY IN HELIOS AND IVOTE

S-*n*	Definition	H	S
S-1	Maximum capacity tests both from a SW and a HW standpoint in environments more demanding than the actual elections to be managed.	X	○
S-2	Specific performance tests for the most critical operations (authentication, encryption, decryption, cryptographic primitives, tallying etc.).	X	○
S-3	Existence of test benches more demanding than the actual elections.	X	○
S-4	Clear indicators and metrics on the max manageable size and complexity from a SW (mathematic/cryptographic capabilities, number of voters) and ex_SW (infrastructure, costs, logistics, second channels etc.) standpoints.	Δ	○
S-5	Type of elections, which can be adequately handled by the *e-voting* system (from consultative referenda to political binding elections).	Δ	○

Evaluation Helios: 4/10 points. Limited to small scale/low risk elections ⩽1.000 ballots.

Evaluation iVote: 9.5/10 points. iVote is one of the very few e-voting systems with a proven track record of managing politically-binding elections with hundreds of thousands of voters involved.

H. Ex-Software Development (ESWD-n)

TABLE VI. EX-SOFTWARE DEVELOPMENT IN HELIOS AND IVOTE

ESWD-*n*	Definition	H	S
ESWD-1	Design, development, and update of SWD/ESWD protocols in parallel.	X	○
ESWD-2	Secure protocol for credential, permission and responsibility distrib.	○	○
ESWD-3	Automated access control and infrastructure surveillance.		○
ESWD-4	Auditing and independent observers' protocol.	Δ	○
ESWD-5	Distributed *back-up* protocol.		○
ESWD-6	Distribution of attributions and responsibilities throughout the whole ex_sw development to minimize collusion risks.	Δ	○
ESWD-7	Availability of complementary, non e-voting systems.	Δ	Δ
ESWD-8	Voters must be informed about the e-voting process in advance, providing communication channels such as websites, telephones, information stands…		○
ESWD-9	If re-voting is permitted, provide a reinforced information campaign to explain the prevalence of paper ballot in any case.		○
ESWD-10	Organization of opinion polls on selected cohorts to gather reliable feedback on usability, tendencies and improvements.		
ESWD-11	Authentication credential submission by alternative channels.	X	○
ESWD-12	Master initialization protocol to be executed right before the start of the e-voting period to verify the correct operation/readiness.	X	○
ESWD-13	Implementation, to the extent possible, of protocolized and standardized systems to improve interoperability.		Δ
ESWD-14	Free assistance phone service available before/during the election.		○
ESWD-15	Complete PR strategy to promote e-voting and train the potential voters, including webinars, stands, demos, open days etc.	Δ	Δ

Helios' academic nature directly affects the available resources and protocols for non-software related aspects. Thus, ESWD-3, ESWD-5, ESWD-8, ESWD-9, ESWD-10, ESWD-13 and ESWD-14 are not applicable. Moreover, the partially compliant ones are evaluated as such because they were specifically implemented for the U. of Louvain pilot [28] but are not available in the standard version [11].

Concerning iVote, the experiences analyzed took place in well-established democracies and with enough resources allocated. In Australia, even additional funds were granted as they were deemed necessary [16]. Accordingly, iVote is compliant with items ESWD-1-ESWD-6, ESWD-8, ESWD-9, ESWD-11, ESWD-12 and ESWD-14. The areas with improvement margin are: additional voting systems, opinion/feedback polls, interoperability and PR strategy.

Evaluation Helios: 3/10 points. The academic origin impacts the available resources.

Evaluation iVote: 9/10 points. iVote's use in Switzerland, Australia and Norway included enough resources and funds to provide a solid policy for non-software related aspects. There is room for improvement in poll/feedback initiatives and PR strategies

I. Incidents and Attacks Protocol (IAP-n)

Coincidentally with (S-n) and (ESWD-n), Helios' origin and scope implies fewer resources available for a proper IAP. Specifically, IAP-1 and IAP-2 are non-compliant while IAP-5 is only partially because the distributed approach is not fully implemented. There is no reference in the official website to aspects related to the rest of the items.

There is no 100% secure system. There are always usability and/or resource-related tradeoffs. As for iVote, the system presents a correct performance for IAP-1, IAP-2, IAP-4 and IAP-5 items. Nonetheless, there were incidents reported in Australia and Norway (albeit no effective attack have been proved). In the case of Neuchâtel, there have been no issues reported. They could improve in the training/awareness campaigns and also by hiring hackers/independent experts to compromise the system beforehand.

TABLE VII. INCIDENTS AND ATTACKS PROTOCOL IN HELIOS/ IVOTE

IAP-*n*	Definition	H	S
IAP-1	*Risk Assessment (RA), Privacy Impact Assessment (PIAS), Penetration Testing (PT), Control Validation Plan (CVP)* and *Control Validation Audit (CVA)* protocols.	X	○
IAP-2	Specific prevention protocols for each cryptographic scheme.	X	○
IAP-3	All the information shall be kept to the extent possible in the country's National soil.		
IAP-4	Implementation of protocols and reinforcement operations to minimize the risk of permanent losses of information.		○
IAP-5	Reinforced distributed approach to contribute to the absence of critical nodes which undermine the e-voting system's viability.	Δ	○
IAP-6	Training and awareness campaigns to minimize the risk of voter-driven attacks (*phishing*, social engineering, etc.).		Δ
IAP-7	Hackers/indep. experts to test and compromise the system beforehand.		Δ

Evaluation Helios: 3/10 + 1 extra point because of the open source approach (transparency) and the limited range of recommended elections.

Evaluation iVote: 8/10 points. iVote shows a solid performance regarding IAP, with clear and detailed protocols, called internally "Business Continuity Plans". Awareness/training campaigns and use of independent experts/hackers are two areas for betterment.

J. Versatility (V-n)

Helios implements neither official versions adapted to different election typolo-gies/cryptographic schemes (V-1) nor specific solutions for vulnerable groups (V-2). The interface is WCAG 2.0 A compliant and it has not been tested in all platforms.

iVote implements solutions adapted to different types of elections [33][16] as well as to vulnerable groups (V-1 and V-2). It is also compliant with V-3 and V-4 but gets an A and not a AA for the WCAG 2.0 standard.

TABLE VIII. VERSATILITY IN HELIOS AND IVOTE

V-*n*	Definition	H	S
V-1	Versions adapted to different election typologies (yes/no, 1/N...).	X	○
V-2	Specific solutions for vulnerable groups (w/disabilities, illiterates etc.).	X	○
V-3	The voter shall be able to vote using her personal device, through a standard internet connection without installing any additional software.	○	○
V-4	E-voting system to be tested in browsers/devices with a market share ≥ 1%.	Δ	○
V-5	The interface is WCAG 2.0 AA compliant.	Δ	Δ

Evaluation Helios: **4/10 points**. V-1 is a relevant aspect, limiting Helios' versatility.

Evaluation iVote: **8/10 points**. Solid but it could adhere better to the design standards.

K. Cost (C-n)

Despite its importance, the cost of implementing e-voting systems is one of the aspects with less bibliography available, partly because most articles tend to focus on the cryptographic/research/security aspects.

Helios' academic origin has been a limitation for some aspects but it implies certain advantages for cost purposes: if we limit its utilization to the recommended range, Helios is a very affordable option (albeit not totally free: there are minimum needs for equipment/human resources), considering its overall performance and quality.

As for iVote, it is difficult to obtain information, partly because they are a private company and also because they have to adapt to each countries' legislation requirements. Scytl is making efforts toward making e-voting tools more affordable but they are still somehow costly. More clarity in the pricing policy would also be appreciated.

TABLE IX. COST IN HELIOS AND IVOTE

C-*n*	Definition	H	S
C-1	Transparency and clarity in the cost breakdown.	○	○
C-2	System cost related to quality and performance. Comparison with other e-voting solutions.	○	Δ

Evaluation Helios: 9/10 points. Not totally free but one of the best option within its range.

Evaluation iVote: 7/10 points. The need to adapt to the idiosyncrasy of each country makes it challenging to define a standard pricing policy. Nonetheless, the website could be more transparent and client-friendly.

L. Maintenance (M-n)

The open source approach of Helios traditionally has allowed the academic com-munity to review and improve the code. Unfortunately In the past years, the researchers have opted for implementing their new proposals in personal projects based on Helios like Belenios [41] or KTV Helios [27], rather than maintaining the original version.

Consequently, Helios' maintenance has not been happening at a desirable pace. Finally, there is no mention to everlasting privacy of its implementation in the website.

With regards to iVote, the amount and diversity of projects under management have kept it updated in both the software and ex-software aspects. With regards to everlasting privacy, albeit partial, several of the most relevant articles have been re-leased by Scytl.

TABLE X. MAINTENANCE IN HELIOS AND IVOTE

M-*n*	Definition	H	S
M-1	Covering both SW and ex_SW aspects. Frequency, thoroughness and existence of security logs to check the maintenance process are also evaluated.	Δ	○
M-2	Maintenance as *everlasting privacy*.		Δ
M-3	Maintenance cost itself.	Δ	○

Evaluation Helios: 5/10 points. Medium performance due to its academic nature and tendency of researchers creating "spin-offs" rather than improving the original version.

Evaluation iVote: 8.5/10 points. iVote presents a strong maintenance policy due to the variety and number of projects developed. Scytl has also been active in everlasting privacy although a bit more effort would be desirable, taking into account the nature of the elections managed.

V. RESULTS

Helios and iVote (Scytl) represent two of the most widely used e-voting tools to date. They both had an academic origin, although Scytl evolved into a private corporation. The protocolized analysis performed in this article aims at clarifying their strengths and weaknesses in order to establish a safe range of utilization. Upon applying [8] to Helios and iVote, the results can be summarized as shown in Table XI.

Regarding the two sine-qua-non properties (E2Ev and CR) representing the five mandatory principles of a democratic election (Council of Europe [9]):

- Helios can be considered E2Ev accepting that: the BB and the authorities are honest and a potential attacker does not compromise Fiat-Shamir [4]. With regards to CR, Helios is not-compliant because there have been reported "ballot stuffing" vulnerabilities.
- iVote is E2Ev according to [32, 33] if there is no collusion among the code-generator, the authentication service and the electoral letter generator, which in practice is very unlike because of the solid role distribution and independent auditing procedures. As for CR, iVote is not compliant because of the implementation of return codes.

TABLE XI. COMPLETE EVALUATION RESULTS FOR HELIOS AND IVOTE

Requirement	Code	Weig	Helios	iVote
E2Ev	E2Ev	N.A.	Δ	Δ
Coerc. Resistance	CR	N.A.	**X**	**X**
Inviolability	(I-*n*)	**1.2**	6 * 1.2 = **7.2**	8 * 1.2 = **9.6**
Usability	(U-*n*)	**0.8**	4 * 0.8 = **3.2**	7.5 * 0.8 = **6**
Monitoring/Audit	(MA-*n*)	**1.2**	4 * 1.2 = **4.8**	8.5*1.2 = **10.2**
Software Devel.	(SWD-*n*)	**1.2**	7.5 * 1.2 = **9**	8.5*1.2 = **10.2**
Scalability	(S-*n*)	**0.8**	4 * 0.8 = **3.2**	9.5 * 0.8 = **7.6**
Ex_Soft. Develop.	(ESWD-*n*)	**1.2**	3 * 1.2 = **3.6**	9 * 1.2 = **10.8**
Incid./AttackProt.	(IAP-*n*)	**1.2**	4 * 1.2 = **4.8**	8 * 1.2 = **9.6**
Versatility	(V-*n*)	**0.6**	4 * 0.6 = **2.4**	8 * 0.6 = **4.8**
Cost	(C-*n*)	**1.0**	9 * 1.0 = **9**	7 * 1.0 = **7**
Maintenance	(M-*n*)	**0.8**	5 * 0.8 = **4**	8.5 * 0.8 = **6.8**
TOTAL		**10**	**51.2**	**82.6**

The open issue with coercion resistance makes both Helios and iVote non-compliant with recommendation 23 of the 2017 Council of Europe guidelines for e-voting [9].

Concerning the quantifiable criteria, divided into 73 items, Helios presents 13 compliances, 26 partial compliances, 17 non-compliances and 17 N.A. It shows a notable performance in software development, cost, and inviolability within its range of use. On the other hand, its academic origin limits the resources in monitoring/auditing, scalability, ex-software development, incidents/attacks protocol and updates. To sum up, Helios is a powerful e-voting tool in two ways:

- As a fully-operative, open source and (internally) auditable " e-voting system, Helios Voting is a valid, almost free of charge option for minor elections in low-risk and low-coercion environments such as universities and professional associations.
- As a good starting platform for e-voting researchers. In fact, there are several examples of prominent e-voting protocols based on Helios such as [27].

Regarding iVote, it obtains 49 compliances, 15 partial compliances, and 9 N.A. Due to its condition as one of the biggest companies in e-voting services with more than 250 professionals and 40 patents, Scytl has a proven track record of successfully managing politically-binding elections in several countries. iVote stands out in software and ex-software development, scalability, versatility, auditing/monitoring and maintenance.

On the downside, there were reported vulnerabilities in Australia and Norway's experiences [3, 32] (although later implementations have taken place without incidences). Additionally, Scytl could improve the usability of iVote to make it more user-friendly and implement a more transparent pricing policy.

VI. CONCLUSION

The ultimate goal of this article is to provide a protocolized source of information and therefore, contribute to the generalization of e-voting in a protocolized and safe way through valuable and efficient evaluation methods for election officials, researchers and voters.

E-voting development should be gradual and preceded by the required legal changes, as included in recommendations no. 27 and 28 by the 2017 Council of Europe on standards for e-voting [9]. The implantation of e-voting solutions needs to be a decision built over firm, technical criteria and analysis rather than political reasons.

Currently, existing shortcomings in Coercion Resistance and usability, together with past security issues even in well tested systems like iVote, advise against a substitution of the traditional suffrage for e-voting technologies.

The authors believe that a more gradual approach, in which e-voting plays an increasing role is the most desirable option. Starting with selected groups of voters (such as foreign residents) in local/regional elections or referenda constitutes the best option to support e-voting while minimizing the risk of successful attacks.

The adoption of evaluation frameworks to analyze e-voting systems/vendors as the one used in the present article can also play an important role to reinforce security in a global landscape where political disputes are increasingly translated into the digital battleground.

REFERENCES

[1] D. Springall, T. Finkenauer, Z. Durumeri, J. Kitcat, H. Hursti, M. MacAlpine, J.A. Halderman: Security Analysis of the Estonian Internet Voting System. Proc. 21st ACM Conf. Comput. Commun. Secur. 12, 2014.

[2] U. S. V. Foundation, "The future of voting," The Future of Voting, 2015. [Online]. Available: https://www.usvotefoundation.org/e2e-viv/summary

[3] "The FREAK attack," The FREAK Attack, 2015. [Online]. Available: https://censys.io/blog/freak

[4] Bernhard, D., Pereira, O., Warinschi, B.: How Not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios. In: ASIACRYPT 2012: Beijing, China, Proceedings. Springer Berlin 2012. pp. 626-643.

[5] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman, "Attacking the Washington, D. C. internet voting system," in Proc. Int. Conf. Financial Cryptography Data Security, 2012, pp. 1–18

[6] VSSC/1622, "IEEE VSSC/1622: Common data format for election equipment," 2015. [Online]. Available: http://grouper.ieee.org/groups/1622/ .

[7] S. R. Neumann, "Evaluation and improvement of internet voting schemes based on legally-founded security requirements," Technische Universitat Darmstadt.

[8] Luis Panizo Alonso, Mila Gasco, David Yeregui Marcos del Blanco, Jose Angel Hermida Alonso, Hector Alaiz Moreton. "E-voting system evaluation based on the Council of Europe recommendations: Helios Voting", IEEE Transactions on Emerging Topics in Computing, 2018.

[9] T. Standards, "Guidelines on the implementation of the provisions of recommendation CM/Rec(2017)5 on standards for e-voting," Proc. 1289th Meet. Ad hoc Comm. Expert. Leg. Oper. Tech. Stand. e- voting, 2017, pp. 1–19.

[10] D. Marcos del Blanco: Cybersecurity applied to the e-democracy: Cryptographic analysis and development of a practical evaluation methodologyforivotingsystems,http://ciberseguridad.unileon.es/archivos/documentos/tesis/Tesis_David_Y_Marcos.pdf, 2018.

[11] B. Adida, "Helios: Web-based open-audit voting," in Proc. 17th Conf. Security Symp., 2008, pp. 335–348.

[12] Scytl SA, https://www.scytl.com/en/.

[13] R. A., K. Braunlich, R. Grimm, and P. Richter, "Sichere Internetwahlen Ein rechtswissenschaftlich-informatisches Modell."

[14] R. A. V. Hammer, and U. Pordesch, KORA. Betriebliche Telefon und ISDN-Anlagen rechtsgema€ss gestaltet. 1993.

[15] The Common Criteria Recognition Agreement, "Common criteria for information technology security evaluation part 1: Introduction and general model july 2009," Nist, vol. 49, no. Jul, 2009, Art. 93.

[16] "Electoral commision New South Gales," 2017. [Online]. Available: http://www.elections.nsw.gov.au/voting/ivote

[17] D. Simic-Draws, et al., "Holistic and law compatible IT security evaluation: Integration of common criteria, ISO 27001/IT-Grundschutz and KORA," vol. 7, 3, 2013 pp. 16-35.

[18] L. Goodman: Snowball Sampling. Ann. Math. 32, 148–170 (1961).

[19] L. Kish: Sample Design in business research. [American Statistical Association, Taylor & Francis, Ltd.].

[20] J. D. C. Benaloh, R. Rivest, P. Y. A. Ryan, P. Stark, V. Teague, and P. Vora, "End-to-end verifiability," arXiv, 2014

[21] D. Bernhard, S. Neumann, and M. Volkamer, "Towards a practical cryptographic voting scheme based on malleable proofs," in Proc. 4th Int. Conf. E-Voting Identify, 2013, pp. 176–192.

[22] D. Zissis and D. Lekkas, Design, Development, and Use of Secure Electronic Voting Systems. Hershey, PA, USA: IGI Global, 2014.

[23] T. T. Taiwhenua, "The department of internal affairs - online voting,"[Online]. Available: https://www.dia.govt.nz/online-voting

[24] S. Kremer, M. Ryan, and B. Smyth, "Election verifiability in electronic voting protocols," in Proc. Eur. Symp. Res. Comput. Security, 2010, pp. 389–404.

[25] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in Proc. Trustworthy Elect., 2010, pp. 37–63.

[26] "Helios voting web." [Online]. Available: https://vote.heliosvoting.org/ .

[27] O. Kulyk, V. Teague, and M. Volkamer, "Extending helios towards private eligibility verifiability," in Proc. 5th Int. Conf. E-Voting Identity, 2015, pp. 57–73.

[28] B. Adida, O. De Marneffe, O. Pereira, et al., "Electing a university president using open-audit voting: Analysis of real-world use of Helios," in Proc. Conf. Electron. Voting Tech., 2009, pp. 1–15.

[29] S. Haber, J. Benaloh, and S. Halevi, "The Helios e-voting demo for the IACR," in Proc. Helios, 2010, pp. 1–7.

[30] V. Cortier, "Formal verification of e-voting: Solutions and challenges," in Proc. ACM SIGLOG, vol. 2, no. 1, 2015, pp. 25–34.

[31] K. Sako, J. Kilian: Receipt-free mix-type voting scheme - A practical solution to the implementation of a voting booth, 1995.

[32] Summary: Expert Study Mission Report The Carter Center Internet Voting Pilot : Norway's 2013 Parliamentary Elections, 2014.

[33] K. Gjøsteen: The Norwegian internet voting protocol. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 7187 LNCS, 2012, pp. 1-18.

[34] M. Hirt, K. Sako: Efficient Receipt-free Voting Based on Homomorphic Encryption. In: Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques. Springer-Verlag, Berlin, 2000, pp.539-556.

[35] C. Z. Acemyan, P. Kortum, M. D. Byrne, and D. S. Wallach, "From error to error: Why voters could not cast a ballot and verify their vote with Helios, Pret a voter, and scantegrity II," USENIX J. Elect. Technol. Syst., vol. 3, no. 2, 2015, pp. 1-25.

[36] S.G. Castell: Individual Verifiability in Electronic Voting.

[37] C. Bull, H. Nore, S. Guasch, J. Puiggal: Internet Voting in Europe : Norway and Switzerland case studies, 2016, pp. 1-14.

[38] C. Burton, C. Culnane, S. Schneider: Secure and Verifiable Electronic Voting in Practice: the use of vVote in the Victorian State Election, 2015.

[39] V. Cortier and B. Smyth, "Attacking and fixing Helios: An analysis of ballot secrecy," J. Comput. Secur., vol. 21 1, 2013, pp 89-148.

[40] V. Cortier, D. Galindo, S. Glondu, and M. Izabachene, "Election verifiability for helios under weaker trust assumptions," in Proc. Eur. Symp. Res.Comput. Security, 2014, pp. 327–344.

[41] S. Glondu: Belenios specification. 1–8 (2013).